UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

BRUCE BAILEY, individually and on behalf of all others similarly situated, Plaintiff, v. PROGRESS SOFTWARE CORPORATION and PENSION BENEFIT INFORMATION, LLC d/b/a PBI RESEARCH SERVICES, Defendants.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Bruce Bailey ("Plaintiff"), through his undersigned counsel, brings this action against Progress Software Corporation ("PSC") and Pension Benefit Information, LLC d/b/a PBI Research Services ("PBI", collectively "Defendants") pursuant to the investigation of his attorney, personal knowledge as to himself and his own acts and otherwise upon information and belief, and allege as follows:

INTRODUCTION

1. PSC is a software company that creates and markets software and applications primarily geared toward businesses. One of those applications is a file transfer software called "MOVEit."

2. PBI is a company that markets services to pension funds and insurance companies. These services largely encompass helping to locate individuals for those

companies and funds. It uses MOVEit to transfer the sensitive personal information ("SPI") of the clients and beneficiaries of those companies and funds.

3. Numerous companies and entities have come forward since mid-June 2023 to announce that the SPI of their clients or (in the case of government records) residents had been stolen. These include the Lousiana Office of Motor Vehicles, the Oregon Department of Transportation, the California Public Employees Retirement System ("CalPERS"), Genworth Finance, Wilton Reassurance, the Tennessee Consolidated Retirement System, and the National Student Clearinghouse. At the time of this writing, new companies and entities continue to come forward to indicate that their information has been stolen as well.

4. For the purposes of this complaint, on or about June 22, 2023, CalPERS announced publicly that on June 16, 2023, PBI had been the recipient of a hack and exfiltration of SPI involving approximately 770,000 individuals who are and have been members of the pension fund (the "Data Breach"). However, the total number of individuals affected by the Data Breach, as of this writing, is at least 15 million individuals.[1]

5. CalPERS reported that this SPI included at least "First and Last Name; Date of Birth; and Social Security Number. It could have also included the names of former or current employers, spouse or domestic partner, and child or children. The information that

[1] *See* https://techcrunch.com/2023/06/29/millions-affected-moveit-mass-hacks/, last accessed July 5, 2023.

was taken involves anyone who was receiving an ongoing monthly benefit payment as of this spring."[2]

6. Various online sources have identified the hacker group responsible as CL0P, a Russian ransomware group "known for asking for multi-million dollar ransoms."[3]

7. CL0P are also identified as having been behind the recent Accellion and Fortra data breaches, both huge breaches the subject of ongoing litigation.[4]

8. Plaintiff and Class members now face a present and imminent lifetime risk of identity theft, which is heightened here by the potential loss of Social Security numbers.

9. The information stolen in cyber-attacks allows the modern thief to assume victims' identities when carrying out criminal acts such as:

- Filing fraudulent tax returns;
- Using your credit history;
- Making financial transactions on behalf of victims, including opening credit accounts in victims' names;
- Impersonating victims via mail and/or email;
- Impersonating victims in cyber forums and social networks;
- Stealing benefits that belong to victims; and
- Committing illegal acts which, in turn, incriminate victims.

10. Plaintiff's and Class members' SPI was compromised due to Defendants' negligent and/or careless acts and omissions and the failure to protect the SPI of Plaintiff

---

[2] https://www.calpers.ca.gov/page/home/pbi, last accessed July 5, 2023
[3] https://www.linkedin.com/pulse/moveit-what-you-need-know-cve-2023-25708-critical-fault-llc/, last accessed July 5, 2023
[4] https://www.databreaches.net/hackers-using-moveit-flaw-to-deploy-web-shells-steal-data/, last accessed July 5, 2023.

and Class members.

11. As of this writing, there exist many class members who have no idea their SPI has been compromised, and that they are at significant risk of identity theft and various other forms of personal, social, and financial harm. The full extent of the Data Breach is not yet known. The risk will remain for their respective lifetimes.

12. Plaintiff brings this action on behalf of all persons whose SPI was compromised as a result of Defendants' failure to: (i) adequately protect consumers' SPI, (ii) adequately warn its current and former customers and potential customers of its inadequate information security practices, and (iii) effectively monitor its platforms for security vulnerabilities and incidents (the "Class"). Defendant's conduct amounts to negligence and violates state statutes.

13. Plaintiff and similarly situated individuals have suffered injury as a result of Defendants' conduct. These injuries include: (i) lost or diminished inherent value of SPI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their SPI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (iv) the continued and certainly an increased risk to their SPI, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the SPI.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

15. This Court has personal jurisdiction over Defendants because Defendant PBI's principal place of business is located within this District.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District. Defendant PBI resides within this judicial district and a substantial part of the events giving rise to the claims alleged herein occurred within this judicial district.

PARTIES

17. Plaintiff Bruce Bailey is a natural person residing in the city and county of Highland, California. On or about June 25, 2023, Plaintiff was informed by letter that he had been a victim of the Data Breach.

18. Defendant Pension Benefit Information, LLC. is a for-profit Delaware corporation with its principal place of business at 333 S 7th Street, Suite 2400, Minneapolis, MN 55402.

19. Defendant Progress Software Corporation is a for-profit Delaware corporation with its principal place of business at 15 Wayside Rd., Suite 4, Burlington, MA 01803.

FACTUAL ALLEGATIONS

20. PSC states that, with its software, a company can "can build what you need, deploy where and how you want, empower your customers, then manage it all safely and securely."

21. PSC created and developed the MOVEit Secure File Transfer application, of which PSC says, "MOVEit enables your organization to meet compliance standards, easily ensure the reliability of core business processes, and secure the transfer of sensitive data between partners, customers, users and systems."[5]

22. PSC licenses the MOVEit software (and related hardware) to companies to "securely" transfer sensitive information between parties. In the case of PBI, PBI uses that information to locate individuals in conjunction with insurance or retiree benefits.

23. In the ordinary course of doing business with PBI, customers (such as CalPERS) provide Defendant with their customer's, client's, or resident's SPI including at least:

a. Contact and account information, such as names, addresses, telephone number, email address, and household members;

b. Authentication and security information such as government identification and/or Social Security number; and

c. Demographic information, such as age, gender, and date of birth;

24. On or about June 6, 2023, PBI began notifying its customers, such as CalPERS that a "previously unknown "zero-day" vulnerability in their MOVEit Transfer Application" allowed CalPERS "data to be downloaded by an unauthorized third party."[6]

---

[5] https://www.ipswitch.com/moveit?_ga=2.209339218.1747267376.1688579744-398139942.1688579744, last accessed July 5, 2023.

[6] https://www.calpers.ca.gov/page/home/pbi, last accessed July 5, 2023.

25. Notably, PBI's website is not as specific, stating that "[a]t the end of May, Progress Software identified a cyberattack in their MOVEit software that did impact a small percentage of our clients who use the MOVEit administrative portal software resulting in access to private records. This incident did not gain access to PBI's core systems or software."[7]

26. Notably, while not explicitly stated by PBI, PBI noted that it uses a "MOVEit Transfer server"[8] which PSC identifies as an "on-premises solution".[9] This means that the MOVEit server was used on the premises of the company using the software, not hosted directly by PSC. As such, PBI appears to have had control of the server in question that was breached.

27. PSC's response to the Data Breach is buried in its Community Articles section, and states that "Progress has discovered a vulnerability in MOVEit Transfer that could lead to escalated privileges and potential unauthorized access to the environment. If you are a MOVEit Transfer customer, it is extremely important that you take immediate action as noted below in order to help protect your MOVEit Transfer environment."[10]

---

[7] https://www.pbinfo.com/faq-communication/, last accessed July 5, 2023.
[8] *Id.*
[9] https://www.ipswitch.com/moveit?_ga=2.209339218.1747267376.1688579744-398139942.1688579744, last accessed July 5, 2023.
[10] https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023, last accessed July 5, 2023.

28. While the first update from PSC was announced on May 31, 2023, according to Union Bank and Trust, another affected entity, the Data Breach initially occurred on May 29, 2023.[11]

29. However, Critical Fault posted a blog entry on June 23, 2023 that identified the first intrusion as happening on May 27, 2023.[12]

30. However, PBI indicates that it "became aware of the MOVEit compromise on June 2, 2023."[13] This is two days after PSC publicly announced the May 31 software update.

31. Given the intrinsically critical nature of the security fix, it is highly unlikely the PBI did not know of the compromise later than May 31, 2023, when PSC publicized it. Vulnerabilities such as this as routinely reported to clients before or concurrent with their public announcements, and if PBI did not update their systems for two days following the announcement of the vulnerability, this inaction is clearly negligent.

32. It remains unclear at this stage whether the Data Breach of PBI's systems, in particular, occurred prior to or after May 31, 2023.

---

[11] https://apps.web.maine.gov/online/aeviewer/ME/40/893229cd-b658-42aa-bb38-f976a32aae2f.shtml, last accessed July 5, 2023.

[12] https://www.linkedin.com/pulse/moveit-what-you-need-know-cve-2023-25708-critical-fault-llc/, last accessed July 5, 2023.

[13] https://www.pbinfo.com/faq-communication/, last accessed July 5, 2023.

33. Defendants have offered no assistance to Plaintiff and class members in remediating the damage from the Data Breach, leaving any offers of assistance to their clients, such as CalPERS.

34. This response is entirely inadequate to Plaintiff and class members who now potentially face several years of heightened risk from the theft of their SPI and who may have already incurred substantial out-of-pocket costs in responding to the Data Breach.

35. Defendants had obligations created by contract, industry standards, common law, and public representations made to Plaintiff and Class members, to keep their SPI confidential and to protect it from unauthorized access and disclosure.

36. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches in the healthcare industry preceding the date of the breach.

37. Indeed, data breaches, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry, including Defendant.

38. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and

patience to resolve.[14] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[15]

39. The SPI of Plaintiff and members of the Classes was taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the SPI for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

40. Defendant knew, or reasonably should have known, of the importance of safeguarding the SPI of Plaintiff and members of the Class, including Social Security numbers, dates of birth, and other sensitive information, as well as of the foreseeable consequences that would occur if Defendants' data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and members of the Class a result of a breach.

41. Plaintiff and members of the Class now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their SPI.

42. The injuries to Plaintiff and members of the Class were directly and

---

[14] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf, last accessed July 5, 2023.

[15] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

proximately caused by Defendants' failure to implement or maintain adequate data security measures for the SPI of Plaintiff and members of the Class.

43. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

44. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

45. The FTC further recommends that companies not maintain SPI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

46. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

47. Defendants failed to properly implement basic data security practices, and

their failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer SPI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

48. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendants' cybersecurity practices.

49. Best cybersecurity practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

50. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers. However, information such as dates of birth and Social Security numbers are even more attractive to hackers; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

51. The SPI of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[16]

52. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration ("SSA") stresses that the loss of an individual's Social Security number, as is the case here, can lead to

[16] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs, last accessed July 5, 2023.

identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[17]

53. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

54. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[18]

55. Furthermore, as the SSA warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use

[17] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Jun. 2018), https://www.ssa.gov/pubs/EN-05-10064.pdf, last accessed July 5, 2023.

[18] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft, last accessed July 5, 2023.

the old number anymore.

> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[19]

56. Here, the unauthorized access left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential SPI to mimic the identity of the user. The personal data of Plaintiff and members of the Class stolen in the Data Breach constitutes a dream for hackers and a nightmare for Plaintiff and the Class. Stolen personal data of Plaintiff and members of the Classes represents essentially one-stop shopping for identity thieves.

57. The FTC has released its updated publication on protecting SPI for businesses, which includes instructions on protecting SPI, properly disposing of SPI, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

58. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office ("GAO") Report to Congressional Requesters:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[20]

59. Companies recognize that SPI is a valuable asset. Indeed, SPI is a valuable

---

[19] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Jun. 2018), http://www.ssa.gov/pubs/EN-05-10064.pdf, last accessed July 5, 2023.

[20] *See* https://www.gao.gov/assets/gao-07-737.pdf (June 2007) at 29, last accessed July 5, 2023.

commodity. A "cyber black-market" exists in which criminals openly post stolen Social Security numbers and other SPI on a number of Internet websites. The stolen personal data of Plaintiff and members of the Class has a high value on both legitimate and black markets.

60. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

61. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns. Defendant's former and current customers whose Social Security numbers have been compromised now face a real, present, imminent and substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

62. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change — Social Security number, driver license number or government-issued identification number, name, and date of birth.

63. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth

more than 10x on the black market."[21]

64. This is even more true for minors, whose Social Security Numbers are particularly valuable. As one site noted, "The organization added that there is extreme credit value in Social Security numbers that have never been used for financial purposes. It's relatively simple to add a false name, age or address to a Social Security number. After that happens, there is a window for thieves to open illicit credit cards or even sign up for government benefits."[22]

65. Among other forms of fraud, identity thieves may obtain driver licenses, government benefits, medical services, and housing or even give false information to police. An individual may not know that his or her driver license was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud, or until the individual attempts to lawfully apply for unemployment and is denied benefits (due to the prior, fraudulent application and award of benefits).

FACTS SPECIFIC TO PLAINTIFF

66. On or about June 26, 2023, Plaintiff was notified via letter from Defendant dated June 22, 2023 that Plaintiff's SPI had been taken as part of the Data Breach.

67. Plaintiff has spent approximately 20 hours attempting to mitigate the damage caused by the theft of his SPI, and has had considerable anxiety as a result of the Data Breach.

68. Since the time of the Data Breach, Plaintiff has heightened numbers of emails

---

[21] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html, last accessed July 5, 2023.

[22] https://www.identityguard.com/news/kids-targeted-identity-theft, last accessed July 11, 2022.

from various scammers. This activity indicates that his information has been placed into the hands of hackers and has already been sold throughout the dark web.

69. Plaintiff is aware of no other source from which the theft of his SPI could have come. He regularly takes steps to safeguard his own SPI in his own control.

CLASS ACTION ALLEGATIONS

70. Plaintiff brings this nationwide class action pursuant to Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following classes:

> All natural persons residing in the United States whose SPI was compromised in the Data Breach announced by Defendants on or about June 6, 2023 (the "Nationwide Class").

71. The California Subclass is defined as follows:

> All natural persons residing in California whose SPI was compromised in the Data Breach announced by Defendant on or about June 6, 2023 (the "California Subclass").

72. The California Subclass, together with the Nationwide Class, are collectively referred to herein as the "Classes" or the "Class."

73. Excluded from the Class are all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, and all judges assigned to hear any aspect of this litigation and their immediate family members.

74. Plaintiff reserves the right to modify or amend the definitions of the proposed Class before the Court determines whether certification is appropriate.

75. **Numerosity**: The Classes are so numerous that joinder of all members is impracticable. Defendant has, as of this writing, indicated to the U.S. Department of Health and Human Services that the total number of Class Members is at least 15 million. The Classes are readily identifiable within Defendant's records.

76. **Commonality**: Questions of law and fact common to the Classes exist and

predominate over any questions affecting only individual members of the Classes. These include:

a. When Defendants actually learned of the Data Breach and whether their response was adequate;

b. Whether Defendants owed a duty to the Classes to exercise due care in collecting, storing, safeguarding and/or obtaining their SPI;

c. Whether Defendants breached that duty;

d. Whether Defendants implemented and maintained reasonable security procedures and practices appropriate to the nature of storing the SPI of Plaintiff and members of the Classes;

e. Whether Defendants acted negligently in connection with the monitoring and/or protection of SPI belonging to Plaintiff and members of the Classes;

f. Whether Defendants knew or should have known that they did not employ reasonable measures to keep the SPI of Plaintiff and members of the Classes secure and to prevent loss or misuse of that SPI;

g. Whether Defendants have adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendants caused Plaintiff's and members of the Classes damage;

i. Whether Defendants violated the law by failing to promptly notify Plaintiff and members of the Classes that their SPI had been compromised;

j. Whether Plaintiff and the other members of the Classes are entitled to credit monitoring and other monetary relief; and

k. Whether Defendants violated various California state laws.

77. **Typicality**: Plaintiff's claims are typical of those of the other members of the Classes because all had their SPI compromised as a result of the Data Breach due to Defendants' misfeasance.

78. **Adequacy**: Plaintiff will fairly and adequately represent and protect the

interests of the members of the Classes. Plaintiff's counsel are competent and experienced in litigating privacy-related class actions.

79. **Superiority and Manageability**: Under rule 23(b)(3) of the Federal Rules of Civil Procedure, a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Classes is impracticable. Individual damages for any individual member of the Classes are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

80. Class certification is also appropriate under Rule 23(a) and (b)(2) because Defendant has acted or refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Nationwide Class as a whole and as the California Subclass as a whole.

81. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiff and members of the Classes to exercise due care in collecting, storing, using, and safeguarding their SPI;

b. Whether Defendants breached a legal duty to Plaintiff and the members of the Classes to exercise due care in collecting, storing, using, and safeguarding their SPI;

c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information

compromised in the Data Breach; and

e. Whether members of the Classes are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

FIRST CLAIM FOR RELIEF
Negligence
(By Plaintiff Individually and on Behalf of the Nationwide Class)

82. Plaintiff hereby re-alleges and incorporates by reference all of the allegations in paragraphs 1 to 81.

83. Defendants routinely handle SPI that is required of their customers, such as the information to Plaintiff and the Class.

84. By collecting and storing the SPI of its customers, Defendants owed a duty of care to the individuals whose SPI it collected to use reasonable means to secure and safeguard that SPI.

85. Defendants has full knowledge of the sensitivity of the SPI and the types of harm that Plaintiff and Class Members could and would suffer if the SPI were wrongfully disclosed.

86. Defendants knew or reasonably should have known that their failure to exercise due care in the collecting, storing, and using of their customers' clients' SPI involved an unreasonable risk of harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third party.

87. Defendants had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or

disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendants' security protocols to ensure that Plaintiff's and Class Members' information in Defendants' possession was adequately secured and protected.

88. Defendants also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' SPI.

89. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class Members was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

90. Plaintiff and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew of should have known of the inherent risks in collecting and storing the SPI of Plaintiff and the Class, the critical importance of providing adequate security of that SPI, and the necessity for encrypting SPI stored on Defendants' systems.

91. Defendants' own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendants' misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included its decisions not to comply with industry standards for the safekeeping of Plaintiff's and Class Members' SPI.

92. Plaintiff and the Class Members had no ability to protect their SPI that was in, and remains in, Defendants' possession.

93. Defendants were in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

94. Defendants had and continue to have a duty to adequately disclose that the SPI of Plaintiff and Class Members within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their SPI by third parties.

95. Defendants had a duty to employ proper procedures to prevent the unauthorized dissemination of the SPI of Plaintiff and Class Members.

96. Defendants have admitted that the SPI of Plaintiff and Class Members were purposely exfiltrated and disclosed to unauthorized third persons as a result of the Data Breach.

97. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the SPI of Plaintiff and Class Members during the time the SPI was within Defendants' possession or control.

98. Defendants improperly and inadequately safeguarded the SPI of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

99. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect the SPI they had in their possession in the face of increased risk of theft.

100. Defendants, through their actions and/or omissions, unlawfully breached

their duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of SPI.

101. Defendants, through their actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

102. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and Class Members, the SPI of Plaintiff and Class Members would not have been compromised.

103. There is a close causal connection between Defendants' failure to implement security measures to protect the SPI of Plaintiff and Class Members and the harm suffered or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff's and Class Members' SPI was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such SPI by adopting, implementing, and maintaining appropriate security measures.

104. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their SPI is used; (iii) the compromise, publication, and/or theft of their SPI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their SPI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent,

detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their SPI, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the SPI of its employees and former employees in its possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the SPI compromised as a result of the Data Breach for the remainder of Plaintiff's and Class Members' lives.

105. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their SPI, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the SPI in its continued possession.

SECOND CLAIM FOR RELIEF
Breach of Third-Party Beneficiary Contract,
(By Plaintiff Individually and on Behalf of the Nationwide Class)

106. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 81.

107. Upon information and belief, PSC entered into contracts with its government and corporate customers to provide secure file transfer services to them; services that included data security practices, procedures, and protocols sufficient to safeguard the Private Information that was entrusted to it.

108. Upon information and belief, PBI entered into contracts with its government and corporate customers to provide beneficiary search services; services that included data security practices, procedures, and protocols sufficient to safeguard the Private Information that was entrusted to it.

109. Such contracts were made expressly for the benefit of Plaintiff and the Class, as it was their Private Information that Defendants agreed to receive, store, utilize, transfer, and protect through its services. Thus, the benefit of collection and protection of the SPI belonging to Plaintiff and the Class was the direct and primary objective of the contracting parties and Plaintiff and Class Members were direct and express beneficiaries of such contracts.

110. Defendants knew or should have known that if it were to breach these contracts with its customers, Plaintiff and Class Members would be harmed.

111. Defendants breached their contracts with customers by, among other things, failing to adequately secure Plaintiff and Class Members' Private Information, and, as a result, Plaintiff and Class Members were harmed by Defendants' failure to secure their Private Information.

112. As a direct and proximate result of Defendants' breach, Plaintiff and Class Members are at a current and ongoing risk of identity theft, and Plaintiff and Class Members sustained incidental and consequential damages including: (i) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out of pocket" costs incurred due to

actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) diminution of value of their SPI; (vii) future costs of identity theft monitoring; (viii) and the continued risk to their SPI, which remains in Defendants' control, and which is subject to further breaches, so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' SPI.

113. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

114. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

THIRD CLAIM FOR RELIEF
Unjust Enrichment, in the Alternative
(By Plaintiff Individually and on Behalf of the Nationwide Class)

115. Plaintiff hereby re-alleges and incorporate by reference all of the allegations in paragraphs 1 to 81.

116. Plaintiff and Class Members conferred a monetary benefit upon Defendants in the form of storing their SPI with Defendant in such a way that saved expense and labor for Defendant.

117. Defendants appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Defendants also benefited from the receipt of Plaintiff's and Class Members' SPI, as this was used by Defendants to facilitate its core functions.

118. The benefits given by Plaintiff and Class Members to Defendants were to be used by Defendants, in part, to pay for or recoup the administrative costs of reasonable data privacy and security practices and procedures.

119. As a result of Defendants' conduct, Plaintiff and Class Members suffered actual damages in an amount to be determined at trial.

120. Under principles of equity and good conscience, Defendants should not be permitted to retain a benefit belonging to Plaintiff and Class Members because Defendants failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Class Members granted to Defendants or were otherwise mandated by federal, state, and local laws and industry standards.

121. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds or benefits it received as a result of the conduct alleged herein.

FOURTH CLAIM FOR RELIEF
Violation of the California Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq.* – Unlawful Business Practices
(By Plaintiff Individually and On Behalf of the California Subclass)

122. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 81.

123. Defendants have violated Cal. Bus. & Prof. Code § 17200, *et seq*., by engaging in unlawful business acts and practices that constitute acts of "unfair competition" as defined in Cal. Bus. & Prof. Code § 17200.

124. Actions for relief may be brought "by a person who has suffered injury in fact and has lost money or property as a result of the unfair competition." Cal. Bus. & Prof. Code § 17204. Plaintiff herein is a "person" as defined by Cal. Bus. & Prof. Code § 17201, and has lost money or property as a result of the unfair competition.

125. Defendants engaged in unlawful acts and practices with respect to the services and employment it provided to the Subclass by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting the SPI of Plaintiff and the Subclass with knowledge that the information would not be adequately protected; and by storing the SPI of Plaintiff and the Subclass in an unsecure environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendants to take reasonable methods of safeguarding the PII and PHI of Plaintiff and the Classes.

126. As a direct and proximate result of Defendants' unlawful practices and acts, Plaintiff and the Subclass were injured and lost money or property, including but not limited to the money Defendant received for the services provided, the loss of Plaintiff's and the Subclass' legally protected interest in the confidentiality and privacy of their SPI, nominal damages, and additional losses as described above.

127. Defendants knew or should have known that Defendants' data security practices were inadequate to safeguard the SPI of Plaintiff and the Subclass and that the risk of a data breach or theft was highly likely, especially given Defendants' inability to adhere to basic encryption standards and data disposal methodologies. Defendants' actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Subclass.

128. Plaintiff and the Subclass seek relief under Cal. Bus. & Prof. Code § 17200, *et seq.*, including, but not limited to, restitution to Plaintiff and the Classes of money or property that Defendants may have acquired by means of Defendant's unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Defendant because of Defendants' unlawful business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

FIFTH CLAIM FOR RELIEF
Violation of California's Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq.* – Unfair Business Practices
(By Plaintiff Individually and on Behalf of the California Subclass)

129. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 81.

130. Defendants have violated Cal. Bus. & Prof. Code § 17200, *et seq*. by engaging in unfair business acts and practices that constitute acts of "unfair competition" as defined in Cal. Bus. & Prof. Code § 17200.

131. Actions for relief may be brought "by a person who has suffered injury in fact and has lost money or property as a result of the unfair competition." Cal. Bus. & Prof. Code § 17204. Plaintiff is a "person" as defined by Cal. Bus. & Prof. Code § 17201, and has lost money or property as a result of the unfair competition.

132. Defendants engaged in unfair acts and practices by establishing the sub-standard security practices and procedures described herein, by soliciting and collecting the SPI of Plaintiff and the Subclass with knowledge that the information would not be adequately protected, and by storing the SPI Plaintiff and the Classes in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and the Classes. They were likely to deceive the public into believing their SPI was securely

stored, when it was not. The harm these practices caused to Plaintiff and the Subclass outweighed their utility, if any.

133. Defendants engaged in unfair acts and practices by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect SPI of Plaintiff and the Subclass from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and the Classes. They were likely to deceive the public into believing their SPI were securely stored, when they were not. The harm these practices caused to Plaintiff and the Subclass outweighed their utility, if any.

134. As a direct and proximate result of Defendants' acts of unfair practices, Plaintiff and the Subclass were injured and lost money or property, including but not limited to the price received by Defendants for the services, the loss of Plaintiff's and the Subclass' legally protected interest in the confidentiality and privacy of their SPI, nominal damages, and additional losses as described above.

135. Defendants knew or should have known that Defendants' data security practices were inadequate to safeguard the SPI of Plaintiff and the Classes and that the risk of a data breach or theft was highly likely, including Defendants' failure to properly encrypt files containing sensitive SPI. Defendants' actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and the Subclass.

136. Plaintiff and the Subclass seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiff and the Subclass of money or property that the Defendants may have acquired by means of Defendants' unfair business practices, restitutionary disgorgement of all profits accruing to Defendants because of Defendants' unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

SIXTH CLAIM FOR RELIEF
Violation of the California Consumer Privacy Act
Cal. Civ. Code §§ 1798.100, *et seq.* (CCPA)
(By Plaintiff Individually and on Behalf of the California Subclass)

137. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 78.

138. Plaintiff and the members of the California Subclass are consumers as that term is defined in Cal. Civ. Code § 1798.140(g).

139. Defendants are businesses as that term is defined in Cal. Civ. Code § 1798.140(c). Defendants are organized or operated for the profit or financial benefit of their owners. Defendants collect consumers' personal information (including that of Plaintiff and the California Subclass) or such information is collected on Defendants' behalf, and Defendants determine the purposes and means of the processing of consumers' personal information. Defendants are corporations organized or operated for the profit or financial benefit of its owners with annual gross revenues in excess of $25,000,000.

140. The information accessed during the Data Breach constitutes "personal information" as that term is defined in Cal. Civ. Code § 1798.140(o)(1). At a minimum, that information included names, Social Security numbers, dates of birth, marital status, employment status, and wage data related to benefits.

141. Under the CCPA, Defendants had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information that they stored. Cal. Civ. Code § 1798.150(a)(1).

142. Defendants' failure to prevent the Data Breach by implementing and maintaining reasonable security procedures and practices constitutes a breach of their duty under the CCPA.

143. As a result of the Data Breach, the nonencrypted and nonredacted personal information of CCPA Plaintiff and the California Subclass was subject to unauthorized

access and exfiltration, theft, or disclosures. The personal information accessed in the Data Breach was nonencrypted and nonredacted as evidenced by the fact that Defendants were required to provide notification letters under the laws of several states that require notification of unauthorized access to nonencrypted and nonredacted information.

144. Defendant violated section 1798.150(a) of the California Consumer Privacy Act ("CCPA") by failing to prevent Plaintiff's and California Subclass members' nonencrypted and nonredacted SPI from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the SPI of Plaintiff and California Subclass members.

145. As a direct and proximate result of Defendant's acts, Plaintiff and the California Subclass members' SPI was subjected to unauthorized access and exfiltration, theft, or disclosure through Defendant's computer systems and/or from the dark web, where hackers further disclosed Defendant's customers', employees', former employees' and their dependents' SPI.

146. As a direct and proximate result of Defendant's acts, Plaintiff and the California Subclass members were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of California Subclass members' legally protected interest in the confidentiality and privacy of their SPI, nominal damages, and additional losses as described above.

147. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard California Subclass members' SPI and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the California Subclass members.

148. At this time, Plaintiff and California Subclass members seek only actual pecuniary damages suffered as a result of Defendant's violations of the CCPA, injunctive and declaratory relief, attorneys' fees and costs, and any other relief the court deems proper.

149. Concurrently with the filing of this complaint, Plaintiff provided written notice to Defendant identifying the specific provisions of this title he alleges they have violated. Assuming Defendant does not cure the Data Breach within 30 days, and Plaintiff believes any such cure is not possible under these facts and circumstances, Plaintiff intends to amend this complaint to also seek the greater of statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater. *See* Cal. Civ. Code § 1798.150(b).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class Members, request judgment against the Defendant and the following:

A. For an Order certifying the Class as defined herein, and appointing Plaintiff and his counsel to represent the Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class Members' SPI;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

   i. prohibiting Defendants from engaging in the wrongful and unlawful

acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff and Class Members' personal identifying information;

iv. prohibiting Defendants from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database (if, in fact, it does so);

v. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vi. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

vii. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

viii. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

ix. requiring Defendants to conduct regular database scanning and securing checks;

x. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xi. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and

xv. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers.

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For pre- and postjudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY DEMAND

Plaintiff hereby demands a trial by jury on all issues so triable.

DATED: July 5, 2023

Respectfully Submitted,

By: /s/ *Carl V. Malmstrom*
Carl V. Malmstrom
Minnesota Bar Number 0391908

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
111 W. Jackson Blvd., Suite 1700
Chicago, Illinois 60604
Tel: (312) 984-0000
Fax: (212) 686-0114
malmstrom@whafh.com

Attorney for Plaintiff and the Putative Class